

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any **suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Legal Recognition and Enforceability of Smart Contracts under Contract Law in India and International Commercial Practice

DR. E. RAMYA*

ABSTRACT

The rapid growth of digital technology and blockchain innovation has transformed the nature of commercial transactions across the globe. Smart contracts, self-executing digital agreements that operate through blockchain technology, have emerged as an important tool in modern international commerce due to their efficiency, transparency, automation, and reduced dependency on intermediaries. However, the increasing use of smart contracts raises significant legal concerns regarding their recognition, validity, enforceability, jurisdiction, and dispute resolution under existing legal frameworks.

This paper analyses the legal recognition and enforceability of smart contracts under Indian contract law and international commercial practice. It examines the applicability of the Indian Contract Act, 1872 and the Information Technology Act, 2000 in determining the validity of electronically executed agreements. This research further evaluates whether traditional contractual principles such as free consent, lawful consideration, offer and acceptance, and intention to create legal relations can effectively apply to automated blockchain-based contracts. It explores the international legal developments, including the role of UNCITRAL Model Laws and global commercial practices in facilitating cross-border digital transactions. The paper also identifies major challenges associated with smart contracts, including coding errors, cybersecurity risks, lack of regulatory clarity, jurisdictional conflicts, and limitations in dispute resolution mechanisms.

The study concludes that although existing laws in India indirectly support the validity of electronic contracts, there remains a significant need for a specialised regulatory framework to address the unique legal and technological issues surrounding smart contracts. The paper suggests legal reforms and policy recommendations to ensure greater certainty, security, and enforceability in international digital commerce.

Keywords: *Smart Contracts; International Commercial Practice; Digital Contracts; Blockchain Technology; Information Technology Act.*

* Author is an Assistant Professor at Chennai Dr. Ambedkar Government Law College, Pudupakkam, Tamil Nadu, India.

I. INTRODUCTION

The rapid development of technology has significantly transformed the global commercial arena. In recent years, digitalisation, artificial intelligence, and blockchain technology have revolutionised the manner in which commercial transactions are conducted across national boundaries. One of the most important innovations emerging from blockchain technology is the concept of smart contracts. Smart contracts are self-executing digital agreements in which the terms and conditions of a contract are automatically executed through computer code without the direct involvement of intermediaries.¹ These contracts aim to provide greater efficiency, transparency, accuracy, and security in commercial transactions.

The increasing use of smart contracts in international trade, banking, insurance, e-commerce, supply chain management, and financial technology has created new opportunities as well as legal challenges. Unlike traditional agreements, smart contracts operate automatically once predetermined conditions are fulfilled.² This unique feature reduces transaction costs and minimises human intervention. However, it also raises complex legal questions regarding consent, enforceability, jurisdiction, liability, and dispute resolution.

In India, the legal validity of contracts is primarily governed by the Indian Contract Act, 1872, while electronic transactions receive recognition under the Information Technology Act, 2000. Although these legislations indirectly support electronic agreements, there is no specific statutory framework dealing exclusively with blockchain-based smart contracts. Issues such as identification of parties, uncertainty, coding errors, automated execution without human control, and cross-border enforceability continue to challenge existing legal systems.³

At the international level, organisations such as UNCITRAL have introduced model laws to facilitate electronic commerce and digital signatures in global trade. Various countries have also begun recognising blockchain transactions and smart contracts through legislative reforms.

¹ *Influence of Digitalization on Business and Management: A Review on Artificial Intelligence, Blockchain, Big Data Analytics, Cloud Computing, and Internet of Things*, ResearchGate, https://www.researchgate.net/publication/385086203_Influence_of_digitalization_on_business_and_management_A_review_on_artificial_intelligence_blockchain_big_data_analytics_cloud_computing_and_internet_of_things (last visited May 26, 2026).

² Amina Bello *et al.* *Smart Contracts and Their Legal Implications in Financial Transactions*, RESEARCHGATE, https://www.researchgate.net/publication/403251332_Smart_Contracts_and_Their_Legal_Implications_in_Financial_Transactions (last visited May 26, 2026).

³ Vivek Kumar, *Contracts, E-Contracts, Validity of E-Contract and Its Types and Differences Between Contracts and E-Contracts*, 12 IJRASET 1415 (2024).

Nevertheless, the absence of uniform international regulations creates difficulties in resolving disputes arising from cross-border smart contract transactions.⁴

This research paper seeks to examine the legal recognition and enforceability of smart contracts under Indian contract law and international commercial practice. The study analyses the applicability of existing laws in India to smart contracts, evaluates international legal developments, and identifies major challenges in enforcement and dispute resolution. The paper further attempts to suggest legal reforms and policy recommendations necessary for establishing a secure and effective regulatory framework for smart contracts in India and global commerce.

II. CONCEPT AND EVOLUTION OF SMART CONTRACTS

A smart contract is generally defined as a self-executing digital agreement in which the terms and conditions are written in the form of computer code and are automatically executed when predetermined conditions are fulfilled. Unlike traditional paper-based contracts, smart contracts operate through blockchain technology and reduce the need for intermediaries such as banks, brokers, or legal agents.⁵ The term ‘smart contract’ was first introduced by computer scientist and cryptographer Nick Szabo in the 1990s. He described smart contracts as computerised transaction protocols designed to execute the terms of a contract automatically. According to him, smart contracts could combine legal principles with technological automation to reduce fraud, transaction costs, and dependence on third parties.

Although the concept existed theoretically for many years, the practical implementation of smart contracts became possible only after the development of blockchain technology.⁶ Blockchain technology acts as a decentralised digital ledger that records transactions in a transparent, immutable, and secure manner. The emergence of cryptocurrencies, particularly Bitcoin, demonstrated the effectiveness of decentralised digital systems.⁷ However, the introduction of Ethereum in 2015 significantly expanded the use of blockchain technology by enabling programmable smart contracts through decentralised applications. Ethereum allowed developers to create automated agreements capable of executing complex commercial transactions without human intervention.

⁴ Saule Kushybek, *International Legal Regulation of Electronic Document Circulation*, 10 HISTORIA I ŚWIAT (2021).

⁵ R. Kaur, A. Ali & Md Faisal, *Smart Contracts: The Self-Executing Contracts*, in BLOCKCHAIN (2022).

⁶ Zibin Zheng et al., *An Overview on Smart Contracts: Challenges, Advances and Platforms*, 105 FUTURE GENERATION COMPUTER SYSTEMS 475 (2020).

⁷ Venkata Ballamudi, *Blockchain as a Type of Distributed Ledger Technology*, 3 ASIAN J. HUMANITY ART & LITERATURE 127 (2016).

The evolution of smart contracts has transformed various sectors of international commerce and business operations. Initially, smart contracts were primarily associated with cryptocurrency transactions, but their application has now expanded to banking, insurance, supply chain management, real estate, healthcare, intellectual property licensing, e-commerce, and international trade. Businesses increasingly use smart contracts because they offer speed, transparency, accuracy, security, and cost efficiency in commercial transactions.⁸

Despite these advantages, the concept of smart contracts differs significantly from traditional legal contracts. Traditional contracts are drafted in natural language and interpreted by courts based on the intention of parties, whereas smart contracts are written in programming code and executed automatically by computer systems. This distinction creates legal and practical challenges relating to interpretation, consent, enforceability, coding errors, liability, and jurisdiction.⁹

In India, the legal system has gradually recognised electronic transactions through the Information Technology Act, 2000, which grants legal recognition to electronic records and digital signatures. However, Indian law does not specifically define or regulate smart contracts. Therefore, the enforceability of such agreements is generally examined under the principles of the Indian Contract Act, 1872. The absence of a dedicated statutory framework creates uncertainty regarding the legal status of blockchain-based contracts and automated commercial transactions.¹⁰

At the international level, organisations such as UNCITRAL have played an important role in promoting electronic commerce and digital contracting through model laws and international principles. Many countries are now attempting to modernise their legal systems to accommodate blockchain technology and smart contracts. As global commerce increasingly shifts toward digital platforms, smart contracts are expected to become an integral part of future commercial transactions, making it essential for legal systems to adapt to emerging technological developments.¹¹

⁸ Lawrence Emma, *Blockchain and Smart Contracts for Secure and Transparent Transactions* (2024).

⁹ Gergana Varbanova, *Legal Nature of Smart Contracts: Contract or Program Code?*, 1 J. DIGITAL TECH. & L. 1028 (2023).

¹⁰ Dinesh Sagar & Singh, *Smart Contracts in India: Law and Challenges*, 2 INT'L J. CREATIVE & OPEN RSCH. ENG. & MGMT. 1 (2026).

¹¹ Arya Anil, *Critical Analysis on the UNCITRAL Model Laws on E-Commerce*, INT'L J. LEGAL RSCH. & ANALYSIS (2024), <https://www.ijlra.com/public/details/critical-analysis-on-the-uncitral-model-laws-on-e-commerce-by-arya-anil>.

III. LEGAL FRAMEWORK IN INDIA

The legal framework governing smart contracts in India is still evolving. Although India does not presently have specific legislation exclusively regulating blockchain technology or smart contracts, several existing statutes indirectly recognise the validity of electronic and automated agreements. The enforceability of smart contracts in India is mainly determined through the combined application of the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023.¹²

A. Indian Contract Act, 1872

The Indian Contract Act, 1872 forms the foundation of contractual relations in India. Section 10 of the Act provides that agreements become legally enforceable contracts when they are made with free consent of competent parties, for lawful consideration, and with a lawful object. Although the Act was enacted long before the emergence of digital technology and blockchain systems, its general contractual principles continue to apply to smart contracts.¹³ A smart contract must therefore satisfy the following essential elements: a lawful offer and valid acceptance, free consent of parties, lawful consideration and a lawful object, capacity of parties, and intention to create legal relations.

In smart contracts, these elements are executed digitally through computer programming and blockchain mechanisms. The offer and acceptance are generally embedded in coded instructions, and execution occurs automatically when predefined conditions are fulfilled. However, the automated nature of smart contracts creates legal uncertainties regarding interpretation of contractual intent, consent, and allocation of liability in cases of coding errors or system failure.¹⁴

B. Information Technology Act, 2000

The Information Technology Act, 2000 provides legal recognition to electronic records and digital transactions in India. The Act plays a significant role in supporting the validity of electronic contracts and online commercial transactions.¹⁵ Section 4 recognises the legal validity of electronic records; Section 5 grants legal recognition to digital signatures; and

¹² IJLLR JOURNAL, *Smart Contracts: The Need of Legal Implications in India*, IJLLR J. (Sept. 15, 2025), <https://www.ijllr.com/post/smart-contracts-the-need-of-legal-implications-in-india>.

¹³ The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).

¹⁴ *Smart Contracts and Blockchain: Legal Issues and Implications for Indian Contract Law*, ResearchGate, https://www.researchgate.net/publication/356089733_Smart_contracts_and_blockchain_legal_issues_and_implications_for_indian_contract_law (last visited May 27, 2026).

¹⁵ *Hot Topic: Understanding E-Contracts*, Mondaq, <https://www.mondaq.com/india/contracts-and-commercial-law/992626/hot-topic-understanding-e-contracts> (last visited May 27, 2026).

Section 10A validates contracts formed through electronic means, providing that contracts shall not be considered unenforceable merely because they were concluded electronically. These provisions indirectly recognise electronically executed agreements.¹⁶

Although the Act does not specifically mention blockchain or decentralised contracts, it establishes the legal basis for electronic commerce and digital contractual relationships in India. However, the Act was enacted prior to the rise of blockchain technology and cryptocurrency systems. Consequently, it does not adequately address issues such as decentralised execution, self-executing code, automated performance, or cross-border blockchain transactions.

C. Bharatiya Sakshya Adhiniyam, 2023

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 has significantly modernised the law relating to electronic evidence in India. The Act replaces the earlier Indian Evidence Act, 1872 and expressly recognises electronic and digital records as admissible evidence. Section 61 provides that electronic or digital records shall not be denied admissibility merely because they are in electronic form, and that such records possess the same legal effect and enforceability as physical documents.¹⁷ Sections 62 and 63 deal with proof and admissibility of electronic records; Section 63 recognises electronic records stored or produced through computers, communication devices, optical media, magnetic media, or semiconductor memory as admissible evidence subject to statutory conditions.¹⁸

These provisions are highly relevant to smart contracts because blockchain transactions, digital signatures, and automated contractual executions are maintained electronically. Blockchain-generated records may therefore be admissible before Indian courts if the procedural requirements under the Bharatiya Sakshya Adhiniyam, 2023 are satisfied.¹⁹

The modernisation of electronic evidence laws under the Bharatiya Sakshya Adhiniyam strengthens the legal ecosystem for digital commerce and blockchain-based transactions in

¹⁶ *E-Commerce and the Law: A Review of India's Information Technology Act, 2000*, ResearchGate, https://www.researchgate.net/publication/248982867_E-commerce_and_the_law_A_review_of_India%27s_Information_Technology_Act_2000 (last visited May 27, 2026).

¹⁷ *Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023*, ResearchGate, https://www.researchgate.net/publication/391004718_Impact_of_E-Records_as_Evidence_in_the_Judicial_System_under_the_Bharatiya_Sakshya_Adhiniyam_2023 (last visited May 27, 2026).

¹⁸ *Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence under the BSA, 2023*, SCC Online Blog, <https://www.sconline.com/blog/post/2024/10/23/electronic-evidence-in-focus-navigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/> (last visited May 27, 2026).

¹⁹ Maheshwari, Shantanu Garg & Daksh Bainsla, *The New Paper Trail: Proving Your Case Through Electronic Evidence*, Lexology (Mar. 10, 2026), <https://www.lexology.com/library/detail.aspx?g=2d50f5b4-8afb-4ef7-88e0-c251805b5551>.

India. Nevertheless, practical concerns relating to authentication, hash verification, coding integrity, and evidentiary certification still remain significant challenges in smart contract disputes.²⁰

Indian courts have recognised the enforceability of electronic contracts and online transactions in various judicial decisions. Agreements concluded through emails, electronic communication, and online platforms have been upheld, provided the essential contractual requirements are fulfilled.²¹ Although there is limited judicial precedent specifically relating to blockchain-based smart contracts, courts in India have shown a progressive approach toward technological developments and digital evidence. This indicates a possibility of future judicial acceptance of smart contracts within the existing legal framework.²²

D. Regulatory Challenges

India still lacks a specific legal framework governing smart contracts and blockchain-based agreements. Existing laws such as the Indian Contract Act, 1872 and the Information Technology Act, 2000 provide only indirect recognition to electronic contracts, creating uncertainty regarding the enforceability and regulation of smart contracts in India.²³

Another major challenge is consent and contractual intention. Since smart contracts execute automatically through coded instructions, users may not fully understand the technical terms, raising concerns regarding informed consent and liability in cases of coding errors or software defects.²⁴

Jurisdiction and dispute resolution create significant challenges in smart contracts because blockchain transactions operate across borders without fixed territorial control. Determining applicable law, competent courts, and enforcement mechanisms becomes difficult, while limited judicial precedent in India further increases legal uncertainty.²⁵

²⁰ IJLLR JOURNAL, *Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: A Critical Analysis of Judicial Interpretation*, IJLLR J. (Mar. 6, 2026), <https://www.ijllr.com/post/admissibility-of-electronic-evidence-under-the-bharatiya-sakshya-adhiniyam-2023-a-critical-analysis>.

²¹ Diya K.B., *Legal Accountability in Online Commercial Contracts* (Feb. 1, 2026), <https://papers.ssrn.com/abstract=6468899>.

²² Sagar & Singh, *supra* note 10.

²³ Parvejur Rahman & Sagufta Mehnaz, *Legal Issues Relating to Smart Contracts*, INT'L J. MULTIDISCIPLINARY RSCH. (2024), <https://www.ssrn.com/abstract=5054029>.

²⁴ Nivedita Rajesh & Swetha Prabha K., *Contract Law in the Digital Age: AI, Blockchain, and the Future of Legal Consent and Liability*, INT'L J. LEGAL RSCH. & ANALYSIS (2024), <https://www.ijlra.com/details/contract-law-in-the-digital-age-ai-blockchain-and-the-future-of-legal-consent-and-liability-by-nivedita-rajesh-swetha-prabha-k>.

²⁵ *Smart Contracts and Decentralized Justice: Dispute Resolution on the Blockchain*, ResearchGate, https://www.researchgate.net/publication/394734542_Smart_Contracts_and_Decentralized_Justice_Dispute_Resolution_on_the_Blockchain (last visited May 27, 2026).

Cybersecurity and data protection are major concerns. Despite blockchain security, smart contracts remain vulnerable to hacking, coding defects, and unauthorised access, which may cause irreversible financial losses and raise concerns regarding privacy and data protection.²⁶

The uncertain legal status of cryptocurrencies in India complicates the regulation of smart contracts, as many blockchain agreements rely on digital assets for payment and execution. The absence of clear statutory regulation creates legal ambiguity regarding the enforceability of crypto-based smart contracts.²⁷

India urgently needs a comprehensive legal framework for smart contracts and blockchain technology to ensure legal clarity, cybersecurity, effective dispute resolution, and protection for businesses and consumers in the digital economy.²⁸

IV. INTERNATIONAL COMMERCIAL PRACTICE

The rapid development of globalisation and digital commerce has significantly transformed international commercial transactions in recent years. Smart contracts have emerged as an important innovation in international commercial practice due to their ability to automate contractual obligations, reduce transaction costs, enhance transparency, and minimise dependence on intermediaries. The integration of blockchain technology into international trade, banking, insurance, logistics, and financial services has accelerated the global acceptance of smart contracts in commercial activities.²⁹

At the international level, several legal and commercial institutions have recognised the importance of electronic commerce and digital agreements. The UNCITRAL Model Law on Electronic Commerce, 1996 and the UNCITRAL Model Law on Electronic Signatures, 2001 established important international standards regarding the legal recognition of electronic records, digital signatures, and electronically concluded agreements. These instruments

²⁶ *Blockchain Security: Common Issues & Vulnerabilities*, NordLayer, <https://nordlayer.com/blog/blockchain-security-issues/> (last visited May 27, 2026).

²⁷ Editor, *Regulating the Unregulated: India's Legal Conundrum with Cryptocurrencies*, SCC ONLINE (Jan. 23, 2026), <https://www.scconline.com/blog/post/2026/01/23/regulating-unregulated-india-legal-conundrum-cryptocurrencies/>; IJLLR JOURNAL, *supra* note 12.

²⁸ Kehinde Ojadamola Takuro, *Assessing the Legal and Regulatory Implications of Blockchain Technology on Smart Contracts, Digital Identity, and Cross-Border Transactions*, 16 WORLD J. ADVANCED RSCH. & REV. 1426 (2022).

²⁹ *Blockchain-Based Cross-Border Payment Systems: Transforming Global Financial Transactions Through Decentralized Innovation*, ResearchGate (Feb. 14, 2026), https://www.researchgate.net/publication/400718169_Blockchain-Based_Cross-Border_Payment_Systems_Transforming_Global_Financial_Transactions_Through_Decentralized_Innovation.

encourage member states to modernise their domestic laws and promote uniformity in international commercial transactions.³⁰

Many countries have also adopted progressive legal approaches toward blockchain technology and smart contracts. Jurisdictions such as the United States, Singapore, the United Kingdom, and the European Union have initiated legal reforms recognising the enforceability of blockchain-based agreements and digital assets. Some countries have expressly provided statutory recognition to smart contracts and distributed ledger technology within their commercial and financial regulatory frameworks. These developments demonstrate the growing international acceptance of automated digital contracting systems.³¹

In international commercial practice, smart contracts are widely utilised in areas such as international supply chain management, cross-border payments, trade finance, insurance claims processing, intellectual property licensing, and decentralised financial services. Their automated nature enables faster execution of obligations and reduces risks associated with manual processing and human error. Businesses particularly benefit from the transparency and immutability offered by blockchain systems, which enhance trust between parties involved in cross-border transactions.³²

However, despite increasing global adoption, significant legal challenges continue to exist in the international regulation of smart contracts. The absence of a uniform international legal framework creates difficulties concerning jurisdiction, applicable law, taxation, consumer protection, and enforcement of automated agreements. Since blockchain networks operate globally without centralised control, disputes involving smart contracts often raise complex conflict-of-law issues. Different countries follow varying regulatory approaches toward cryptocurrencies, digital assets, and electronic contracts, which further complicates international commercial transactions.³³

³⁰ *Law Relating to E-Commerce: International and National Scenario with Special Reference to India*, ResearchGate (2026), https://www.researchgate.net/publication/338847115_Law_Relating_To_E-Commerce_International_and_National_Scenario_with_Special_Reference_to_India.

³¹ Cansin Ertan, *Enforceability of Blockchain Technologies in Financial Legal Services: The UK and the EU Analysis* (City Univ. of London 2023), https://www.academia.edu/108252842/Enforceability_of_Blockchain_Technologies_in_Financial_Legal_Services_The_UK_and_the_EU_Analysis.

³² *Smart Contracts in Banking and Financial Services: A Qualitative Review of Applications, Risks, and Regulatory Perspectives*, ResearchGate (2026), https://www.researchgate.net/publication/401034496_Smart_Contracts_in_Banking_and_Financial_Services_A_Qualitative_Review_of_Applications_Risks_and_Regulatory_Perspectives.

³³ Atit Kumar, Monika Rastogi & Rajiv Kumar Jha, *The Legal & Regulatory Challenges of Blockchain & Cryptocurrency, Corporate Accountability, Financial Compliance and the Impact of Global Securities Laws*, 8 INTERNATIONAL JOURNAL OF LAW MANAGEMENT AND HUMANITIES 466 (2025).

International arbitration is increasingly emerging as a preferred mechanism for resolving smart contract disputes due to its flexibility, confidentiality, and suitability for cross-border commercial matters. Arbitral institutions and legal experts are now exploring specialised frameworks for blockchain-related dispute resolution and online arbitration systems. Nevertheless, technical complexities relating to coding interpretation, identification of anonymous parties, and enforcement of awards against decentralised entities continue to present practical challenges.³⁴

The international commercial practice indicates a gradual transition toward digital and automated contracting systems supported by blockchain technology. While smart contracts offer substantial advantages in global trade and commerce, effective international cooperation and harmonised legal regulation remain essential to ensure certainty, security, and enforceability in cross-border digital transactions.³⁵

V. CHALLENGES IN ENFORCEMENT

The enforcement of smart contracts presents several legal and practical difficulties despite their growing use in international commercial transactions. Since smart contracts operate through automated computer code on blockchain networks, traditional legal principles are often inadequate to address the unique technological issues arising from such agreements. The absence of clear and uniform legal regulations creates uncertainty regarding the enforceability of smart contracts, particularly in cross-border commercial transactions.³⁶

One of the major challenges relates to the interpretation of contractual terms. Traditional contracts are drafted in natural language and interpreted by courts based on the intention of the parties. In contrast, smart contracts are written in programming code, which may not always accurately reflect the actual intention of the contracting parties. Courts and legal professionals may face difficulties in understanding technical coding language, especially when disputes arise concerning the execution or performance of the contract. Any coding error or software defect

³⁴ *Arbitration in Smart Contracts Disputes – A Look into the Future*, ResearchGate (2026), https://www.researchgate.net/publication/376742095_Arbitration_in_Smart_Contracts_Disputes_-_A_Look_into_the_Future.

³⁵ *Smart Contracts and International Trade: European Legal Strategies for Managing Challenges*, ResearchGate (2026), https://www.researchgate.net/publication/376844579_Smart_Contracts_and_International_Trade_European_Legal_Strategies_for_Managing_Challenges.

³⁶ *Enforcement of Smart Contracts in Cross-Jurisdictional Transactions*, ResearchGate, https://www.researchgate.net/publication/387176520_Enforcement_of_smart_contracts_in_cross-jurisdictional_transactions (last visited May 27, 2026).

may automatically execute unintended transactions, leading to financial losses and contractual disputes.³⁷

Another significant issue is the determination of jurisdiction and applicable law. Smart contracts frequently operate on decentralised blockchain networks that are not confined to any particular territory. Parties involved in a transaction may belong to different countries while the digital infrastructure itself exists globally. This creates uncertainty regarding which country's laws will govern the contract and which court or tribunal will possess jurisdiction in the event of disputes. The absence of harmonised international regulations further complicates enforcement in cross-border transactions.³⁸

The irreversible nature of blockchain transactions also creates enforcement challenges. Once a smart contract is executed on a blockchain network, it is generally impossible to alter or reverse the transaction without consensus from the network participants. While this feature enhances security and transparency, it may also result in injustice where the contract executes incorrectly due to fraud, coercion, technical malfunction, or coding defects. Traditional legal remedies such as rescission, injunction, or rectification become difficult to implement in automated decentralised systems.³⁹

Identification of parties is another major concern in enforcing smart contracts. Blockchain transactions often allow users to operate anonymously or through encrypted digital identities. In cases involving fraud, breach of contract, or illegal transactions, identifying the actual parties responsible becomes highly difficult for courts and enforcement agencies. This anonymity creates obstacles in imposing legal liability and enforcing judicial decisions.⁴⁰

Cybersecurity threats and technological vulnerabilities further affect enforceability. Smart contracts may be exposed to hacking attacks, malware, phishing, and exploitation of coding loopholes. Since these agreements function entirely through software systems, any technical vulnerability may compromise the integrity and security of the transaction. Determining legal

³⁷ Varbanova, *supra* note 9.

³⁸ *Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice*, ResearchGate, https://www.researchgate.net/publication/359558965_Blockchain_Dispute_Resolution_for_Decentralized_Autonomous_Organizations_The_Rise_of_Decentralized_Autonomous_Justice (last visited May 27, 2026).

³⁹ *Examining the Role of Blockchain in Enhancing Transparency and Traceability in Sustainable Supply Chains*, ResearchGate (Apr. 30, 2026), https://www.researchgate.net/publication/399747199_Examining_the_Role_of_Blockchain_in_Enhancing_Transparency_and_Traceability_in_Sustainable_Supply_Chains.

⁴⁰ TOM TIMSIT & ROBERT HERIAN, *LEGAL AND REGULATORY FRAMEWORK OF BLOCKCHAINS AND SMART CONTRACTS* (2019).

responsibility for such technological failures remains a complex issue under existing legal frameworks.⁴¹

There is also limited judicial precedent relating specifically to smart contracts in many countries, including India. Courts are still developing legal approaches toward blockchain technology and automated agreements. The lack of specialised technical expertise among judges, lawyers, and enforcement authorities may further delay effective dispute resolution. Existing procedural laws are also not fully equipped to address the complexities of blockchain evidence and decentralised transactions.⁴²

Although smart contracts offer efficiency, automation, and transparency in commercial transactions, their effective enforcement remains legally challenging. Comprehensive legal reforms, international cooperation, technological safeguards, and specialised dispute resolution mechanisms are essential to ensure certainty and enforceability in the evolving landscape of digital commerce and blockchain-based contractual relationships.⁴³

VI. COMPARATIVE ANALYSIS

The legal recognition and regulation of smart contracts vary significantly across different jurisdictions. While some countries have adopted progressive legal frameworks specifically recognising blockchain technology and smart contracts, others continue to rely upon traditional contract laws and electronic commerce regulations. A comparative analysis of India and other major jurisdictions demonstrates both the progress achieved internationally and the regulatory gaps that still exist within the Indian legal system.⁴⁴

In India, the enforceability of smart contracts is primarily derived from the principles contained in the Indian Contract Act, 1872 and the Information Technology Act, 2000. Indian law recognises electronic contracts and digital signatures, thereby indirectly supporting the validity of smart contracts. However, India does not presently possess a dedicated statutory framework specifically regulating blockchain technology, cryptocurrencies, or self-executing digital agreements. Consequently, the legal status of smart contracts continues to remain uncertain in

⁴¹ Sarwar Sayeed, Hector Marco-Gisbert & Tom Caira, *Smart Contract: Attacks and Protections*, 8 IEEE ACCESS 1 (2020).

⁴² Swati Suman, *Smart Contracts & Indian Law Legally Binding or Technically Blinded*, 11 INTERNATIONAL JOURNAL OF LAW 66 (2025).

⁴³ Sloane Whitaker et al. *Leveraging Smart Contracts to Automate Commercial Agreements and Prevent Disputes*, 6 JOURNAL OF ADVANCED RESEARCH AND TRANSFORMATIVE KNOWLEDGE 355 (2026).

⁴⁴ Madinabonu Yakubova, *Smart Contracts and Their Legal Recognition: Comparative Analysis of Regulatory Approaches*, 3 UZBEK J.L. & DIGITAL POL'Y (2025).

several aspects, particularly regarding liability, jurisdiction, coding errors, and decentralised execution mechanisms.⁴⁵

In contrast, the United States has adopted a comparatively progressive approach toward smart contracts and blockchain regulation. Several states, including Arizona, Tennessee, and Nevada, have enacted laws expressly recognising blockchain technology and smart contracts as legally enforceable agreements. These statutes provide legal validity to electronic records secured through blockchain systems and acknowledge smart contracts as valid methods of conducting commercial transactions. The United States legal framework therefore offers greater certainty to businesses utilising blockchain technology in commercial operations.⁴⁶

Similarly, the United Kingdom has demonstrated a favourable legal approach toward smart contracts through judicial and institutional recognition. The UK Jurisdiction Taskforce issued legal statements recognising crypto-assets and smart contracts under English law. English courts have also shown willingness to interpret and enforce blockchain-based agreements using existing contractual principles. The flexibility of English common law has enabled adaptation to emerging digital technologies without immediate need for extensive statutory reforms.⁴⁷

Singapore has also emerged as a leading jurisdiction in regulating digital commerce and blockchain technology. The country promotes innovation through business-friendly regulations while maintaining strong financial oversight. Singaporean courts and regulatory authorities recognise electronic contracts and digital payment systems, making the jurisdiction attractive for blockchain-based commercial activities and international arbitration involving digital disputes.⁴⁸

The European Union follows a comparatively regulatory-oriented approach. The EU emphasises consumer protection, cybersecurity, financial stability, and data privacy while regulating digital transactions and crypto-assets. Recent initiatives such as the Markets in Crypto-Assets Regulation (MiCA) aim to establish harmonised legal standards for digital assets and blockchain systems across member states. This approach seeks to balance technological innovation with regulatory safeguards.⁴⁹

⁴⁵ IJLLR JOURNAL, *supra* note 12.

⁴⁶ Frank Emmert, *The Regulation of Cryptocurrencies in the United States of America*, 25 EUR. J.L. REFORM 27 (2024).

⁴⁷ Ligia Catherine Arias-Barrera, *The Legal Nature of Tokens: A Functional Typology for an Emergent Asset Class* (Apr. 1, 2026), <https://papers.ssrn.com/abstract=6505558>.

⁴⁸ Lin Lin, *Regulating FinTech: The Case of Singapore*, 35 NUS LAW 94 (2019).

⁴⁹ Luis M. Hinojosa Martínez, *Clearing the crypto-assets wilderness: the EU Commission MiCA proposal*, REVISTA GENERAL DE DERECHO EUROPEO / GENERAL JOURNAL OF EUROPEAN LAW - ISSN 1696-9634 (Oct. 2021), https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=424082.

A comparison of these jurisdictions highlights that India still remains in the early stages of regulating smart contracts and blockchain technology. While Indian law provides partial recognition to electronic agreements, it lacks the clarity and certainty available in several developed jurisdictions. Unlike countries that have introduced express legislative recognition for blockchain transactions, India continues to depend upon traditional contractual principles that may not adequately address the complexities of decentralised automated agreements.⁵⁰

Furthermore, dispute resolution mechanisms in advanced jurisdictions are increasingly adapting to blockchain-related disputes through online arbitration systems and technology-oriented commercial courts.⁵¹ In India, however, there is still limited judicial precedent and institutional preparedness concerning smart contract disputes. This creates practical difficulties in enforcement and interpretation. Comparative analysis therefore demonstrates the urgent need for India to modernise its legal framework in accordance with international developments. By adopting clear regulations relating to smart contracts, digital assets, blockchain evidence, and dispute resolution, India can strengthen legal certainty, promote innovation, and facilitate greater participation in the rapidly expanding global digital economy.

VII. RECOMMENDATIONS

The growing use of blockchain technology and smart contracts in international commerce highlights the urgent need for a modern and comprehensive legal framework in India. Although existing laws like the Indian Contract Act, 1872 and the Information Technology Act, 2000 indirectly recognise electronic agreements, they are insufficient to address the unique legal and technological complexities associated with self-executing smart contracts. India should introduce specific legislation defining the legal status, validity, and enforceability of smart contracts and blockchain-based transactions.

The government should establish proper regulatory guidelines regarding digital signatures, blockchain authentication, electronic consent, and automated execution mechanisms. A uniform legal framework would reduce uncertainty and encourage businesses, investors, and financial institutions to adopt blockchain technology with greater confidence. Special attention must also be given to cross-border transactions by harmonising domestic regulations with international commercial standards and UNCITRAL principles.

⁵⁰ Suman & Das, *supra* note 42.

⁵¹ Xiangbin Zuo et al. *Innovative Dispute Resolution: The Application of Blockchain in Cross-Border E-Commerce Governance*, 3 J. ECOHUMANISM (2024).

India should further strengthen its cybersecurity and data protection framework to address risks associated with hacking, coding vulnerabilities, fraud, and unauthorised access in blockchain systems. Since smart contracts function entirely through software code, regular technical audits and security standards should be made mandatory for blockchain-based commercial platforms. Regulatory authorities should also create mechanisms to determine liability in cases involving coding errors, technical malfunction, or system failure.

India should also develop specialised dispute resolution mechanisms for blockchain and smart contract disputes. Courts, arbitrators, and legal professionals should receive technical training regarding blockchain technology and digital evidence. Online dispute resolution systems and technology-oriented arbitration procedures may provide faster and more efficient remedies in international digital commerce. The admissibility and verification of blockchain records under the Bharatiya Sakshya Adhiniyam, 2023 should also be clarified through judicial guidelines and procedural reforms.

In addition, India should formulate balanced regulations concerning cryptocurrencies and digital assets because many smart contracts rely upon blockchain-based payment systems. A clear regulatory policy would reduce uncertainty while simultaneously protecting consumers, investors, and financial stability. Consumer awareness and digital literacy programmes should also be promoted to ensure that users understand the legal and technological implications of smart contracts before entering into automated agreements.

VIII. CONCLUSION

Smart contracts represent a significant technological advancement in the field of international commerce and digital business transactions. Their ability to automate contractual obligations, reduce transaction costs, enhance transparency, and eliminate intermediaries has transformed the modern commercial landscape. The integration of blockchain technology into global trade, banking, insurance, and financial services demonstrates the growing importance of smart contracts in the evolving digital economy.

In India, existing legal frameworks such as the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023 provide partial legal recognition to electronic contracts and digital evidence. However, the absence of dedicated legislation specifically regulating smart contracts creates significant legal uncertainty regarding enforceability, liability, jurisdiction, cybersecurity, and dispute resolution. Traditional legal principles are often inadequate to address the complexities arising from decentralised and self-executing blockchain systems.

International developments indicate that several countries have already adopted progressive legal approaches toward blockchain technology and smart contracts. Comparative analysis reveals that India must modernise its regulatory framework to remain competitive in the rapidly expanding global digital economy. Effective legal reforms and international cooperation are essential to establish certainty, security, and uniformity in digital commercial transactions.

While smart contracts offer substantial benefits for businesses and international trade, their successful implementation depends upon the creation of a balanced and technologically adaptable legal framework. A comprehensive regulatory approach would not only promote innovation and economic growth but also ensure protection of contractual rights, consumer interests, and legal accountability in the digital era.
